
毕业设计（论文）

设计（论文）题目：**Linux 系统下 VPN 技术分析**

摘 要

网络技术迅猛发展，网络的规模越来越大。从局域网、广域网到全球最大的互联网，从封闭式的、自成体系的网络系统环境到开放式的网络系统环境，这一切无不说明人们在面临着网络技术迅猛发展的同时，也面临着对网络建设的挑战。如何根据自身需求规划、设计网络系统，选择什么样的网络系统、拓扑结构、服务器、客户机、网络操作系统和数据库软件，由哪些供应商提供以上所说的网络系统的软硬件支持，如何开发网络上的应用系统，使其充分发挥网络系统的作用，取得应有的经济效益，这已不仅涉及简单的部件组合，而且需要技术和管理知识有机结合起来，其已成为当前网络建设中亟待解决的问题。

本文主要为深入分析 IPsec 协议体系，研究 IPsec 的工作原理和工作的流程。并且将进一步研究 IPsec 在 Linux 环境中的实现机制，在 linux 的环境下搭建一个简单高效的基于 IPsec 的 VPN 连接。

【关键词】 虚拟专用网 VPN IPsec Linux OpenSWAN 安全证书

ABSTRACT

With the development of network technology, the scale of network is more and more large. The advance from LAN, WAN to the world's largest Internet and the improvement of the open network environment give us all kinds of knowledge, at the same time, which led people faced with more challenge. According to our own requirements for network, we choose a kind of network system, topology structure, server, client, network operating system and database software. In addition, what kind of suppliers also need people to decide. However, how to develop the network application system, make it give full play to the role of network system, obtain economic benefit is not only simple combination, but also a organic combination with technology and management knowledge which become the current problem to be solved in network construction.

This paper mainly analyse the IPsec agreement system: study the work principle and procedure of IPsec; research in the realization mechanism of IPsec in Linux; build a simple and efficient connection of VPN based on IPsec in Linux.

【Key words】 VPN Ipsec Linux OpenSWAN Certificate

目 录

前 言.....	1
第一章 VPN 概述.....	3
第一节 VPN 的定义.....	3
一、VPN 的优缺点分析.....	3
第二节 VPN 分类.....	5
一、按接入方式分.....	5
二、按协议实现类型分.....	5
三、按 VPN 发起方式分.....	6
四、按 VPN 服务类型分.....	7
五、按承载主体分.....	8
第三节 VPN 的连接方式.....	9
一、传输模式.....	9
二、隧道模式.....	9
第四节 VPN 关键技术.....	10
一、隧道技术.....	10
二、加解密技术.....	10
三、密钥管理技术.....	10
四、身份认证技术.....	11
第五节 本章小结.....	11
第二章 IPsec 概述.....	12
第一节 IPsec 简介.....	12
一、IPsec 提供的服务.....	12
二、IPsec 具有以下特点：.....	13
三、封装模式.....	13
四、IPsec 优缺点.....	14
第二节 IPsec 协议体系.....	15
一、IPsec 基本工作原理.....	16
二、安全关联.....	18
三、AH 头认证.....	20
四、ESP 简介.....	23
第三节 因特网密钥交换 IKE.....	25

一、IKE 定义	25
二、IKE 的消息格式	26
第四节 本章小结	29
第三章 Linux 下基于 IPsec 的 VPN 实施	30
第一节 设计目标	30
一、目标	30
二、平台选择以及工具使用	30
三、基于 IPsec 支持的 linux 内核编译	33
第二节 认证与配置网络模型为	40
一、设计的网络模型	40
二、RSA Signature（RSA 数字签名）认证的配制	41
三、x.50Array 证书认证的配置	44
第三节 本章小结	49
结 论	50
致 谢	51
参考文献	52
附 录	53
一、英文原文	53
二、英文翻译	58

前言

随着当今社会的不断发展，网络技术可谓无所不在，信息技术的高速发展和信息量的飞速膨胀，让诞生于 70 年代的 Internet 得以快速的发展。到现在无论是公司还是个人办公，都越来越离不开网络，许多企业和政府机构纷纷将自己的局域网连入 Internet，然而，扩大的网络环境也带来了一系列的问题：随着企业的不断扩大，分支机构越来越多，合作伙伴越来越多，公司的移动用户也越来越多，企业希望能通过无处不在的因特网来实现方便快捷的访问企业的内部网络，更好的处理办公。此时，经济又安全的企业间的互联的 VPN 便脱颖而出托。它恰好能很好的适应企业的需求，又在安全性有很好的加密算法。

目前，国内企业内部的信息化程度都越来越高，很多公司都建有自己的局域网，并且部署了例如财务系统、ERP 系统和 OA 系统等等，可是建设和维护一个提供远程基础数据传输所需的昂贵费用却使绝大多数企业望而却步，如果采用 DDN (Digital Data Network, 数字数据网) 专线方式，昂贵的网络运营费用将给企业带来沉重的思想负担。它们只能通过远程拨号访问或简单的 FTP 传输等手段来维系不同地域信息系统之间数据交换的最低要求，这些都严重制约了信息系统整体效能的发挥。虽然 Internet 为企业实现数据访问提供了方便，但它的高度开放性和松散管理结构也让企业面临严重的网络安全问题。当下，企业迫切需要一种低成本的网络互联解决方案，以提供企业的异地分支机构和合作伙伴或移动用户与公司总部之间畅通、安全地交换或共享业务数据。

当代，网络技术迅猛发展，网络的规模也越来越大。从最小的局域网、广域网到全球最大的互联网 Internet，从封闭式的、自成体系的网络系统环境到开放式的网络系统环境，这一切无不都在说明人们在面临着网络技术迅猛发展的同时，也面临着一个对网络建设的挑战。如何根据自身需求规划、设计网络系统，选择什么样的网络系统、拓扑结构、服务器、客户机、网络操作系统和数据库软件，由哪些供应商提供以上所说的网络系统的软硬件支持，如何开发网络上的应用系统，使其充分发挥网络系统的作用，取得最好的经济效益，这已不仅涉及简单的部件组合，而且需要技术和管理知识有机结合起来，已成为当前网络建设中亟待解决的问题。

DDN 技术虽然可以实现企业间互连，但租金昂贵；ADSL 宽带虽然价格低廉，但其只能应用于企业接入 Internet，不能实现企业之间的互联。由于安全意识淡薄，同时又缺乏应有的安全防范措施，使得公司网络被非法入侵、数据被篡改和窃听等事件时常发生。虽然一些企业采取了一些相应的安全措施如建立自己的防火墙等，但是据报道有 1/3 的防火墙已被黑客攻破，许多安全措施也形同虚

设。为了防止非法用户进入内部网络对数据进行存取和窃听，必须认真解决验证对方身份、防止抵赖、确保数据的真实性和完整性等安全问题。

那么，有没有一种接入方式既可以访问 Internet，又可以实现企业互连，同时接入费用低廉的方式呢？

为此，各种的网络安全技术和产品应运而生，其中 VPN（Virtual Private Network，虚拟专用网）及其相关技术经过多年的实践、发展和完善，最终凭借它的方便性、安全性、标准化、成本低等优势脱颖而出，逐步成为现代企业实现网络跨地域安全互联的主要技术手段，是目前和今后一段时间内企业构建广域网络的发展趋势，据有关研究机构统计，企业通过使用 VPN 的费用能比专用网节省 60% 的资金。

虚拟专用网 VPN 技术早在 1993 年，欧洲虚拟专用网联盟（EVUA）就成立了，当时并力图在全欧洲范围内推广 VPN。Internet 的迅猛发展为 VPN 提供了技术基础，为全球化的企业提供了 VPN 市场，这些都使得 VPN 开始遍布全世界。特别是最近几年，VPN 以迅猛发展之势博得了众多用户的喜爱和好评。

企业实际构建虚拟专用网络需要对一系列与互通和安全相关的问题作出决策，如 VPN 技术和产品的选用、用户认证、私有 IP 地址的分配和传送、NAT、流量控制等等。

本文的第一章对 VPN（虚拟局域网）做了一些基本概念和实际应用中的介绍。第二章深入研究和阐述了 IPsec 协议的体系结构，包括安全协议 AH 和 ESP，IKE（密钥管理协议）和安全关联 SA 等。第三章着重介绍了在 Linux 环境下部署基于 IPsec 的 Net-to-Net 的 VPN，并详细的描述了 IPsec 的配置和安全证书的创建，配置和管理。

第一章 VPN 概述

第一节 VPN 的定义

VPN(Virtual Private Network)，即虚拟专用网络。“虚拟”的概念是相对传统私有网络的构建方式而言的，“虚拟”的含义是指在开放，不安全的网络环境中利用加密，认证等安全技术构建专用，安全的通信信道，从而模拟出一个“私用”的网络^[1]。

VPN 的定义为，VPN 是一种运载加密或认证的可通信的网络，数据在 VPN 中的传输是安全的，其安全性由加密，认证等安全技术来保证，其传输是通过开放的，非安全的公用网络。

VPN 的作用：企业通过公网实现跨地域的系统互联必然面临安全问题。使用公用网络会导致机构间的传输信息容易被窃取，同时攻击者有可能通过公网对机构的内部网络实施攻击，因此需要在企业间建立安全的数据通道，该通道应具备以下的基本安全要素：保证数据真实性；保证数据完整性；保证数据的机密性；提供动态密钥交换功能和集中安全管理服务；提供安全防护措施和访问控制等。VPN 即能有效解决这些安全问题。

一、VPN 的优缺点分析

1、VPN 的优缺点

几年前，很多人都认为 VPN 将逐渐被一些更高级的网络安全技术和价格更便宜的广域网取代，并将随着技术更新而逐渐淘汰。但是，就目前市场调查来看，VPN 技术强大的安全性，高可靠与低成本却一直在今天吸引着企业的目光，越来越多的企业开始重新评估 VPN 服务。下面就 VPN 的优缺点进行简单的分析。

（1）、VPN 的优点：

①节约成本

通过公用网来建立 VPN 与建立 DDN、PSTN 等专线方式相比，可以节省大量的费用开支。VPN 的最大吸引力是价格。相对于传统的广域网而言，VPN 能够在现有的公网中直接实现连接，比传统广域网连接远程用户更加便捷，且运营成本几乎为零。有调查指出，如果 VPN 产品替代传统的组网方式，可以节约

大量的运营成本，甚至会达到 60%到 80%。这是由于 VPN 是在 Internet 上临时建立的安全专用虚拟网络，用户就节省了租用专线的费用，在运行的资金支出上，除了购买 VPN 设备，企业所付出的仅仅是向企业所在地的 ISP 支付一定的上网费用，也节省了长途电话费，故 VPN 价格更低廉。

②高安全性

VPN 能够提高水平的安全，私用身份识别和加密协议避免数据受到劫持和修改，能够很好的阻止数据窃取和替他非授权用户接触这些数据，所以 VPN 能够保证内部机密数据的安全性，保证不同用户使用权限的可控性，能够保证用户信息交换的安全和可靠。使用 VPN 之后，内部网络的重要数据可以在不被侵扰的情况下经过加密后进行路线传输并安全的存储。同时还可以有效的对内部资源的使用者进行权限控制管理。并记录所有的重要的通信过程

③高速

VPN 能够让公司远程员工，合作伙伴或者其他授权的用户利用本地的高速宽带连接链接到企业的内部网络中。

④高灵活性

现代企业的组织结构和商业活动非常灵活，用户如果想与合作伙伴联网，如果没有 VPN，双方的信息技术部门就必须协商如何在双方之间建立租用线路或帧中继线路，有了 VPN 之后，只需双方配置安全连接信息即可；当不再需要联网时，也很方便拆除连接。使用 VPN 可以保持企业工作人员在任何情况下都能够快速的和安全的完成信息内部的交换，并且能够根据企业不断发展的网络规模迅速的扩展自己。

⑤完全控制主动配置

企业可以利用公网或在网络内部自己组建管理 VPN，由自己负责用户的查验、访问权、网络地址配置、安全性和网络变化管理等重要工作。

（2）、VPN 的缺点：

①非直接可控

由于 VPN 是基于互联网的，企业不能直接控制它的可靠性和性能，并且多数企业需要依靠提供 VPN 服务的互联网服务提供商保证服务运行

②建设难度高

目前，多数企业选择有互联网服务提供商负责运行维护的 VPN，而非自己创建和部署。主要原因是 VPN 网络建设需要高水平的理解网络和安全问题，需要认真的规划和配置。

③设备兼容性差

多数厂商不愿意或者不能遵守 VPN 技术标准,不同厂商的 VPN 产品和解决方案通常是不兼容的,混合使用不同厂商的产品可能会出现技术问题,由此可能导致增加企业成本。

④管理复杂

VPN 组网以后,随着企业内部网络范围扩大了,管理问题会比较多。

第二节 VPN 分类

根据不同的需要,可以构建不同类型的 VPN;不同的角度,VPN 的分类也不相同;不同的厂商在销售 VPN 产品的时候,使用了不同的方式的分类;不同的 ISP (Internet Service Provider, 互联网服务提供商) 在开展 VPN 业务时推出了不同的分类方式,用户往往可以根据自己需求划分 VPN^[1]。

一、按接入方式分

这是用户和运营商最关心的 VPN 划分方式。通常情况下,用户可能是通过专线或者拨号上网。

1、专线 VPN

由运营商根据客户需求,专门建设一条用于 VPN 通信的通道。他能一直在线,通过专线接入 ISP 边缘路由器的用户提供 VPN 解决方案

2、拨号 VPN

是一种可以按照用户需求连接的 VPN,它是利用拨号分组交换数据网 PSTN 或者综合业务数字网 ISDN 接入 ISP 的用户提供 VPN 业务,可以节省用户的长途费用。

二、按协议实现类型分

这是 VPN 厂商和 ISP 最关心的划分方式。简单的说 VPN 是通过公共网络连接的两个端点,在它们之间建立一条逻辑连接。逻辑连接可以是在 OSI (Open

system interconnection,开放系统互连)模型的第二层或第三层建立,根据逻辑连接模型,将VPN技术划分成第二层VPN和第三层VPN

1、第二层 VPN

运行在 OSI 参考模型的第二层,他们是点到点的,通过虚电路在场点之间建立连接性。虚电路是网络中两个端点之间的逻辑端到端连接,可以跨越网络中的多个网络原件和物理网段。ATM 和帧中继是两种最流行的第二层 VPN 技术,另外包括 PPTP (点到点隧道协议), L2F (第二层转发协议), L2TP (第二层隧道协议)等

2、第三层 VPN

递送报头位于 OSI 模型的第三层,常见的第三层 VPN 包括通用路由封装 GRE,多协议标签交换 MPLS 和互联网协议安全 IPsec VPN。第三层 VPN 可以以点到点的方式连接两个场点,如 GRE 和 IPsec,也可以在众多场点之间建立全互连连接性,如 MPLS VPN

①、通用路由封装 (Generic Routing Encapsulation, GRE)

最早是由 Cisco 开发的一种 VPN 技术, Cisco 将 GRE 作为一种封装方法开发,是指一个协议的数据包可以封装进 IP 数据包中,并且将封装后的数据包通过 IP 骨干传输。

②、因特网协议安全 (IPsec)

IPSec 不是某种特殊的加密算法或认证算法,也没有在它的数据结构中指定某种特殊的加密算法或认证算法,它只是一个开放的结构,定义在 IP 数据包格式中,为目前流行的数据加密或认证的实现提供了数据结构,为这些算法的实现提供了统一的体系结构,这有利于数据安全方面的措施进一步发展和标准化。同时,不同的加密算法都可以利用 IPSec 定义的体系结构在网络数据传输过程中实施。

③、多协议标签交换 (Multi-Protocol Label Switching, MPLS)

指定了数据吧是如何通过一种有效的方式送到目的地的,是一种用户快速数据包交换和路由的体系。相对于其它 VPN 技术, MPLS VPM 的重要优点在于灵活性,他允许在 VPN 场点之间采用任何网络拓扑。

三、按 VPN 发起方式分

这是客户和 ISP 最关心的 VPN 分类.

1、客户发起

VPN 服务提供的起始点和终止点是面向客户的，其内部技术构成，实施和管理对 VPN 客户可见。需要客户和隧道服务器方案装隧道软件。此时 ISP 不需要做支持建立隧道的任何工作。经过对用户身份符和口令的验证，客户方和隧道服务器极易建立隧道。双方也可以用加密的方式通信。

2、服务器发起

在公司中心部门或 ISP 处理安装 VPN 软件，客户无需安装任何特殊软件，其内部构成，实施和管理对 VPN 客户完全透明。

四、按 VPN 服务类型分

根据服务类型，VPN 业务可以分为三类，接入 VPN，内联网 VPN 和外联网 VPN。

1、企业内部 VPN（Intranet VPN）

在 VPN 技术出现以前，公司两异地机构的局域网想要互联一般会采用租用专线的方式，虽然该方式也采用隧道等技术，在一端将数据封装后通过专线传输到目的方解封装，然后发往最终目的地。该方式也能提供传输的透明性，但是它与 VPN 技术在安全性上有根本的差异。而且在分公司增多、业务开展越来越广泛时，网络结构趋于复杂，费用昂贵。利用 VPN 特性可以在 Internet 上组建世界范围内的 Intranet VPN。利用 Internet 的线路保证网络的互联性，而利用隧道、加密等 VPN 特性可以保证信息在整个 Intranet VPN 上安全传输。Intranet VPN 通过一个使用专用连接的共享基础设施，连接企业总部、远程办事处和分支机构。企业拥有与专用网络的相同政策，包括安全、服务质量(QoS)、可管理性和可靠性。

2、扩展的企业内部 VPN（Extranet VPN）

此种类型由于是不同公司的网络相互通信，所以要更多地考虑设备的互联，地址的协调，安全策略的协商等问题。利用 VPN 技术可以组建安全的 Extranet，既可以向客户、合作伙伴提供有效的信息服务，又可以保证自身的内部网络的安全。Extranet VPN 通过一个使用专用连接的共享基础设施，将客户、供应商、合作伙伴或兴趣群体连接到企业内部网。企业拥有与专用网络的相同政策，包括安

全、服务质量(QoS)、可管理性和可靠性。

3、远程访问 VPN（Access VPN）

与传统的远程访问网络相对应，在该方式下远端用户不再是如传统的远程网络访问那样，通过长途电话拨号到公司远程接入端口，而是拨号接入到用户本地的 ISP，利用 VPN 系统在公众网上建立一个从客户端到网关的安全传输通道。这种方式最适用于公司内部经常有流动人员远程办公的情况。出差员工拨号接入到用户本地的 ISP，就可以和公司的 VPN 网关建立私有的隧道连接，不但保证连接的安全，同时负担的电话费用大大降低。

五、按承载主体分

这是客户和 ISP 最关心的问题。客户一般会自建 VPN 或外包 VPN，这通常决定由建设 VPN 的成本，复杂度等多方面的决定。

1、自建 VPN

企业在驻地安装 VPN 的客户端软件，在企业网边缘安装 VPN 网关软件，完全独立于运营商建设自己的 VPN 网络，运营商不需要做任何对 VPN 的支持工作。选择之间 VPN 的客户，一般资金充足，拥有相当的专业技术力量，而且在安全性等方面对网络有特殊要求，需要自行控制 VPN 网络。另外，用户和站点分布范围广，数量较多，对保密和可用性有一定要求，而对实时业务要求不高的中小企业，还有在内部网中止键 VPN 部门的子网企业，也需要自建 VPN。

2、外包 VPN

用户将 VPN 及远程外包给某一服务提供商，用户将得到安全策略管理，用户管理以及获得技术支持。企业可以因此降低组建和运维 VPN 的费用，而运营商也可以因此开拓新的 IP 业务增值服务市场，获得更好的收益，并提高客户的保持力和忠诚度。

第三节 VPN 的连接方式

一、传输模式

传输模式连接用于在设备的真正源和目的 IP 地址之间传输数据时使用。

传输模式是使用封装方法，防火墙将 UDP 段封装在 VPN 的数据包或者段里面；VPN 封装包含的信息将帮助目标设备确认被保护的信息；VPN 信息接着会封装进一个 IP 数据包，而源设备是防火墙，目标设备是系统日志服务器。

二、隧道模式

传输模式的一种限制是它不具备很好的扩展性,因为保护是基于每一台设备的。因此，当更多的设备需要在两个不用区域以安全的方式相互通信时，应该使用隧道模式。在隧道模式中，实际的源和目标设备通常不保护流量，相反，某些中间设备用于保护这些流量。代表其他设备提供 VPN 保护的设备通常被称呼为 VPN 网关

隧道模式的封装过程，区域的防火墙产生一个系统日志信息，将它封装到一个 UDP 中，并放入 IP 数据包；当 VPN 网关收到区域 PIX 的系统日志 IP 数据包后，VPN 网关会封装整个带有 VPN 保护信息的数据包；接着，VPN 网关将这个信息放入到另一个 IP 数据包中。

模式 协议	传输模式	隧道模式
AH	IP —AH—Data	IP—AH—IP—Data
ESP	IP—ESP—Data—ESP-T	IP—ESP—IP—Data— ESP-T

图 1.1 传输模式与隧道模式的报头区别

第四节 VPN 关键技术

一、隧道技术

隧道技术是 VPN 的基础技术，也是 VPN 的核心技术。它类似于点对点连接技术，在公网建立一条数据隧道，让数据包通过这条隧道传输。它将原始数据包进行加密，信息结构变换，协议封装和压缩后，嵌入另一种协议数据包后在网络中传输，使得只有被授权的用户才能对隧道中的数据包进行解释和处理，且隧道是专用的，从而保护远程用户或主机和专用网络之间的连接，

1、隧道技术在 VPN 的实现中具体有如下主要作用

- ①一个 IP 隧道可以调整任何形式的有效负载，是远程用户能够透明的拨号上网来访问企业的 IP
- ②对倒能够利用封装技术同时调整多个用户或多个不同形式的有效负载。
- ③使用隧道技术访问企业网时，企业网不会向公网报告它的 IP 地址
- ④隧道技术允许接收者滤掉或报告个人的隧道连接。

二、加解密技术

加密技术是数据通信中一项较为成熟的技术。利用加密技术保证传输数据的安全是 VPN 安全技术的核心。为了适应 VPN 的工作特点，目前 VPN 均采用对称加密体制和公钥加密体制相结合的方法。

对称密钥使用同一把钥匙来对信息提供安全的保护。因为同一把要是用于建立和检查安全保护，该算法相对比较简单而且非常有效率。因此，对称算法，工作速度非常快。VPN 目前常用的对称密码加密算法有：DES，3DES，RC4，RC5 等

公钥加密体制，或非对称加密体制，是通信各方使用的两个不同的密钥，私钥被源安全的收藏，永远都不会和其他的设备共享，公钥可以送给其他设备。非对称密钥可以用于加密数据和执行验证功能。当前常见的公钥体制有 RSA

三、密钥管理技术

密钥管理技术的主要任务是如何实现在公用数据网上安全的传递密钥而不会被窃取。密钥管理包括，从密钥的产生到密钥的销毁的各个方面。主要表现于管理体制，管理协议和密钥的产生，分配，更换和注入

密钥的分发有两种方法:1 通过手工配置的方式.2 采用密钥交换协议动态分发, 适合于复杂网络的情况, 而且密钥可快速更新, 可以显著提高 VPN 的应用的安全性。

四、身份认证技术

身份认证是为了保证操作者的物理身份与数字身份相对性,它是防护网络资产的第一道关口。VPN 需要解决的首要问题就是网络上用户与设备的身份认证,如果没有一个万无一失的身份认证方案,不管其他安全设施有多严密。整个 VPN 功能都将失效。身份认证技术可划分为非PKI 身份认证和 PKI 体系身份认证

第五节 本章小结

本章主要从 VPN 的定义,分类以及在架构 VPN 服务器中所用到的相关技术,做了详细的分析,这些在实际现实的架构中,为 VPN 的建设提供了实用的认知的指导,也为我在下面的建设 VPN 的时候,知道了会用到的相关技术,例如数据的加密,解密,证书的管理等。本章中,在介绍 VPN 的优缺点时,我们理性的了解到,VPN 在给我们巨大方便的同时,仍然存在某些的不足。事务都具有两面性,在运用 VPN 时,如何来规避一些它自身的缺点,从而为用户带来更好的体验,是我们研究的方向。章节中还具体分析了 VPN 在实际生活中的分类,我们可以通过自己或企业的具体需求,规划自己的 VPN。根据不同的 VPN,也可以了解到,他们之间的区别,以及和 IPS 运营商之间的联系,这些都可以使在实际的建设中带来方便。安全,是现在互联网上最值得大家关注的对象,VPN 的安全也不例,VPN 说到底,还是要在公网上传播数据的,如何保证这些数据的安全性,这对任何一个架设 VPN 的同学都是令人感到头疼的事情,世上没有绝对安全的东西,但是我们不能不对 VPN 做安全管理。本章中,介绍了 VPN 建设中所用到的一些隧道技术,安全技术,最大的保障了 VPN 数据在传送过程中的安全性。能做到一个高效的,安全的,稳定的连接,才是我们最终所要用到的 VPN。

第二章 IPsec 概述

第一节 IPsec 简介

IPsec (IP Security) 是 IETF 制定的三层隧道加密协议, 它为 Internet 上传输的数据提供了高质量的、可互操作的、基于密码学的安全保证。

IPSec 不是某种特殊的加密算法或认证算法, 也没有在它的数据结构中指定某种特殊的加密算法或认证算法, 它只是一个开放的结构, 定义在 IP 数据包格式中, 为目前流行的数据加密或认证的实现提供了数据结构, 为这些算法的实现提供了统一的体系结构, 这有利于数据安全方面的措施进一步发展和标准化 [11]。同时, 不同的加密算法都可以利用 IPSec 定义的体系结构在网络数据传输过程中实施。

IPSec 协议是一个应用广泛、开放的 VPN 安全协议。IPSec 适应向 Ipv6 迁移, 它提供所有在网络层上的数据保护, 进行透明的安全通信。IPSec 提供了如何使敏感数据在开放的网络 (如 Internet) 中传输的安全机制。IPSec 工作在网络层, 在参加 IPSec 的设备 (如路由器) 之间为数据的传输提供保护, 主要是对数据的加密和数据收发方的身份认证。

一、IPsec 提供的服务

1、数据机密性 (Confidentiality)

IPsec 发送方在通过网络传输包前对包进行加密。

2、数据完整性 (Data Integrity)

IPsec 接收方对发送方发送来的包进行认证, 以确保数据在传输过程中没有被篡改。

3、来源认证 (Data Authentication)

IPsec 在接收端可以认证发送 IPsec 报文的发送端是否合法。

4、防重放（**Anti-Replay**）

IPsec 接收方可检测并拒绝接收过时或重复的报文。

二、IPsec 具有以下特点：

- （1）支持 IKE（Internet Key Exchange，因特网密钥交换）
可实现密钥的自动协商功能，减少了密钥协商的开销。可以通过 IKE 建立和维护 SA 的服务，简化了 IPsec 的使用和管理。
- （2）所有使用 IP 协议进行数据传输的应用系统和服务都可以使用 IPsec，而不必对这些应用系统和服务本身做任何修改。
- （3）对数据的加密是以数据包为单位的，而不是以整个数据流为单位，这不仅灵活而且有助于进一步提高 IP 数据包的安全性，可以有效防范网络攻击

三、封装模式

1、隧道（**tunnel**）模式

用户的整个 IP 数据包被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。通常，隧道模式应用在两个安全网关之间的通讯。

2、传输（**transport**）模式

只是传输层数据被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被放置在原 IP 包头后面。通常，传输模式应用在两台主机之间的通讯，或一台主机和一个安全网关之间的通讯 [4]。

不同的安全协议在 tunnel 和 transport 模式下的数据封装形式如图2.1所示，data 为传输层数据。

协议 \ 模式	传输模式	隧道模式
AH	IP —AH—Data	IP—AH—IP—Data
ESP	IP—ESP—Data— ESP-T	IP—ESP—IP—Data— ESP-T

图2.1传输模式与隧道模式的封装情况

四、IPsec 优缺点

1、IPsec 的优点

- ①IPsec 工作在传输层之下，因此对应用层是透明的，当在路由器或者防火墙上安装 IPsec 时，无需要更改用户或服务器系统中的软件设置。即使在终端系统中执行 IPsec，应用程序等上层软件也不会受影响。另外，IPsec 也可以为单个用户提供主机到主机的安全隧道，保护客户的敏感信息。IPsec 选择在 IP 成是一种很好的选择，更好级别的服务只能保护某一种协议，更低级别的服务则只能保护某一种通信媒体，而 IPsec 则可以保护 IP 之上的任何协议和 IP 之下的任何通信媒体。
- ②IPsec 具有模块化的设计，即使选择不同的算法，也不会影响到其他部分的实现，不同用户群可以根据自己的需求选择合适的算法集
- ③IPsec 使用包过滤的方式进行访问控制。则按可以减少握手的时间，一次握手就可以传送大量的数据，尤其适用于传输数据量大的应用
- ④VPN 交换机的分离通道特性为 IPsec 客户端提供同时对 internet，extranet 和本地网络访问的支持，该技术可以设置权限，允许用户的访问权限，如允许本地打印和文件共享访问，允许直接 internet 访问和允许安全外网访问，该特性使用用户在安全条件下合理方便的使用网络资源，既有安全性又有灵活性。

IPsec 定义了开放的体系结构和框架。

2、IPsec 的缺点

IPSec 需要已知范围的 IP 地址或固定范围的 IP 地址，因此在动态分配地址时不太适合于 IPSec；除了 TCP/IP 协议以外，IPSec 不支持其它协议；除了包过滤外，它没有指定其它访问控制方法；对于采用 NAT 方式访问公共网络的情况难以处理；IPSec 目前还仅支持单播的(Unicast)IP 数据包，不支持多播(Multicast)和广播(Broadcast)的 IP 数据包^[14]。

第二节 IPsec 协议体系

下图 为 体系结构

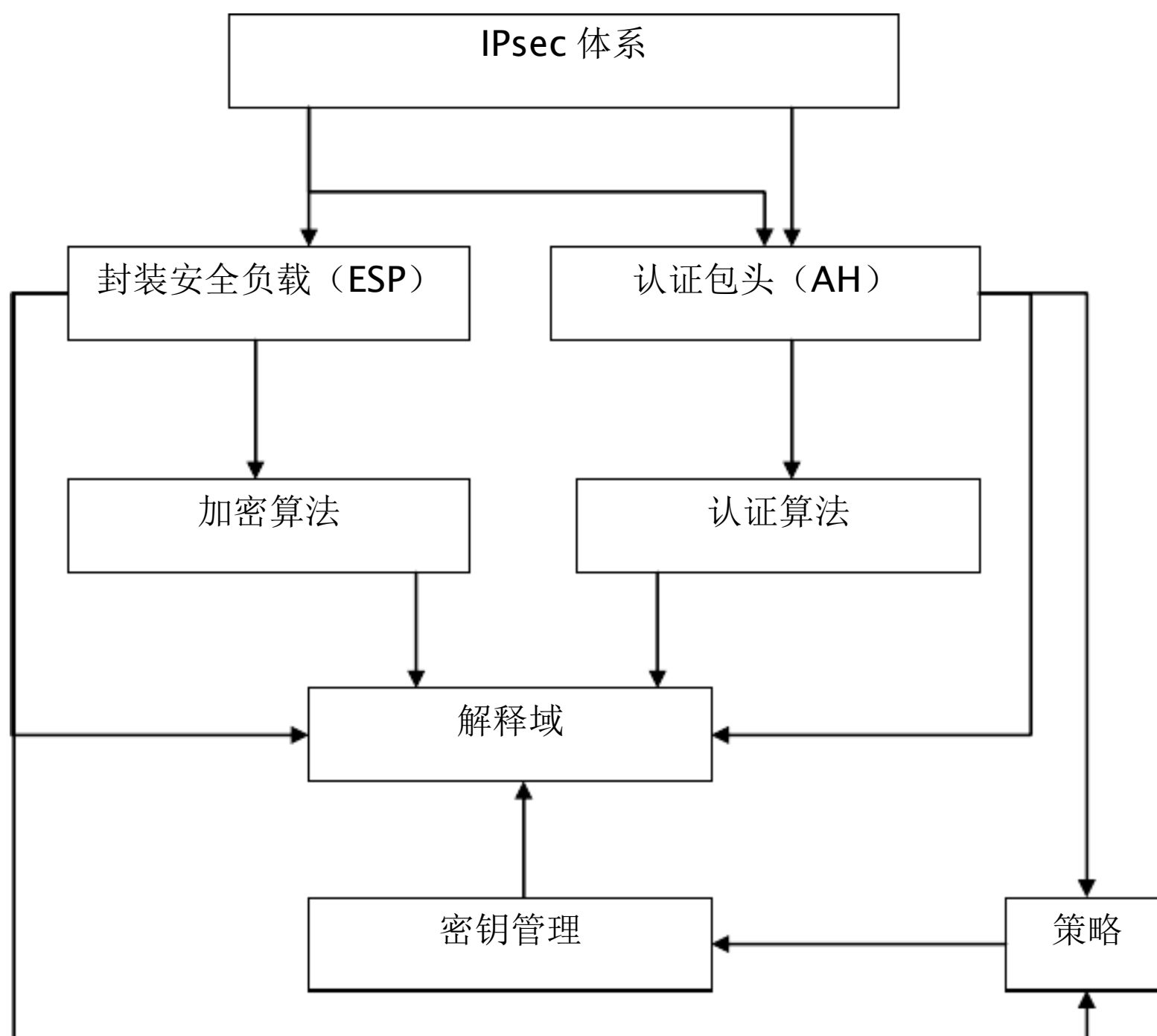


图 2.2 Ipec 协议体系

(1)IPsec 体系文档是 RFC2401，它定义了 IPsec 的基础结构，指定 IP 包的机密性和身份认证使用的传输安全协议 ESP 或 AH 实现，包好了一半的概念，安全需求，定义和定义 IPsec 的技术机制。

(2)ESP（Encapsulate Serurity Payload，封装安全载荷），定义了为通信提供机密性，完整性保护和抗重播服务的额具体实现方法，以及 ESP 头在 ESP 实现中应插入 IP 头的位置，ESP 载荷格式，各字段的语义，取值方式以及对进入分组和外出分组的处理过程。

(3)AH（Authentication Header，认证头），定义了为通信提供完整性和看重放服务的具体实现方法，以及 AH 头在 AH 实现中应插入 IP 头的位置，

AH 头的语法格式，各字段的语义，取值方式以及实施 AH 时对进入和外出分组的处理过程。

(4)认证算法，定义了对 ESP 的认证算法为散列函数 MD5 或 SHA 的 HMAC 版本。

(5)加密算法，定义了 DES-CBC 作为 ESP 的加密算法以及如何实现 DES-CBC 算法和初始化矢量的生成。

(6)IKE (Internet Key Exchange, 因特网密钥交换), 定义了 IPsec 通信双方如何动态建立共享安全参数和经认证过的密钥。IKE 的功能包括: 加密/鉴别算法和密钥的协商, 密钥的生成, 交换及管理, 通信的模式保护, 密钥的生存期等。

(7)IPsec DOI (Domain of Interpretation, 解释域), IKE 定义了安全参数如何协商, 以及共享密钥如何建立, 但没有定义协商内容, 协商内容与 IKE 协议本身分开实现。协商的内容被归于一个单独的文档内, 名为 IPsec DOI

(8)策略, 是两个实体间通信的规则, 它决定采用什么协议, 什么加密算法和认证算法来通信, 策略不当可能造成不能正常工作。

一、IPsec 基本工作原理

IP 协议本身不继承任何安全特性, 在传输过程中很容易伪造 IP 包的地址, 修改其内容, 重播以前的包, 以及拦截并查看包的内容^[2]。因此, 在 internet 上传递 IP 数据包可能会遇到身份欺骗, 数据的完整性破坏, 数据的隐私性破坏等安全威胁。

IPsec 可以有效的保护 IP 数据包的安全, 主要采取的保护形势为: 数据源验证, 无连接数据的完整性验证, 数据内容的机密性, 抗重播保护等。比如, AH 或 ESP 协议进行身份认证的保护, 也可以进行数据完整性的保护。使用 ESP 或 AH 协议, 可以对 IP 数据包或三层协议进行保护, 其中, AH 可以认证数据的起源地, 保障数据的完整性以及防止相同数据包的重播。ESP 除具有 AH 的所有能力之外, 还可以选为数据流提供机密性保障。

IPsec 虚拟隧道接口对报文的加封装/即封装发生在隧道接口上^[8]。用户流量到达实施 IPsec 配置的设备后, 需要 IPsec 处理的报文会被转发到 IPsec 虚拟隧道接口上进行加封装/接封装。

接口加封装如下图 2.3

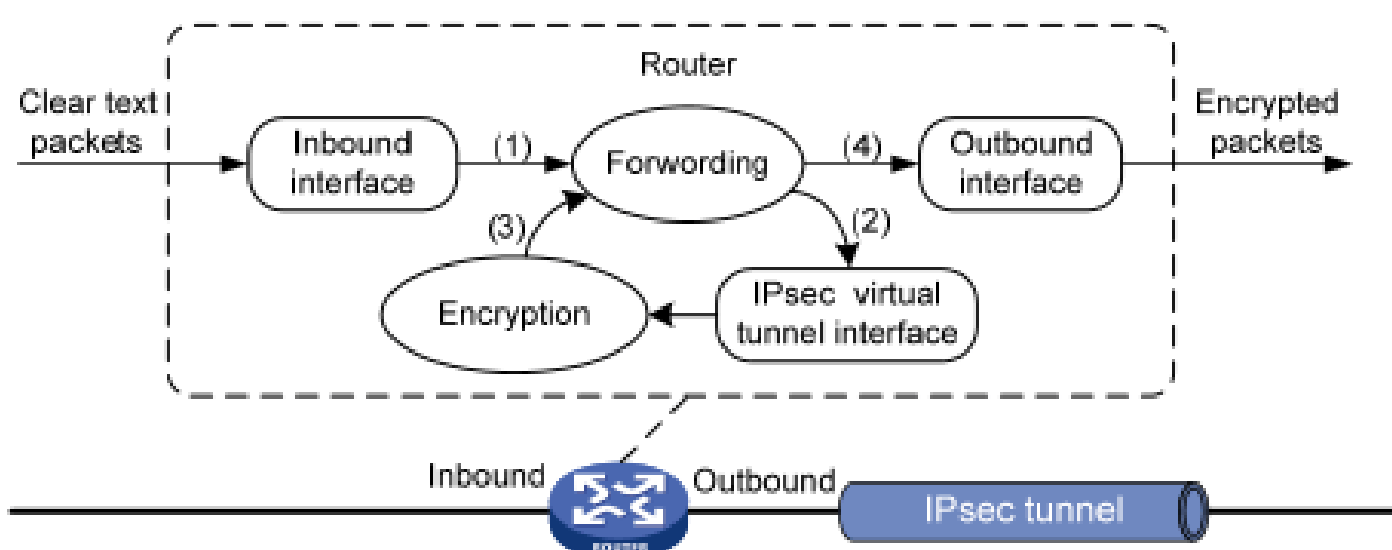


图 2.3 IPsec 虚拟隧道接口对报文进行加封装的过程

- (1) Router 将从入接口接收到的 IP 明文送到转发模块进行处理；
- (2) 转发模块依据路由查询结果，将 IP 明文发送到 IPsec 虚拟隧道接口进行加封装，原始 IP 报文本封装在新的 IP 报文中，新的 IP 头中的源地址和目的地址分别为隧道接口的源地址和目的地址
- (3) IPsec 虚拟隧道接口完成对 IP 明文的加封装处理后，将 IP 密文送到转发模块进行处理。
- (4) 转发模块进行第二次路由查询后，将 IP 密文通过隧道接口的实际物理接口转发出去

接口解封装如下图 2.4

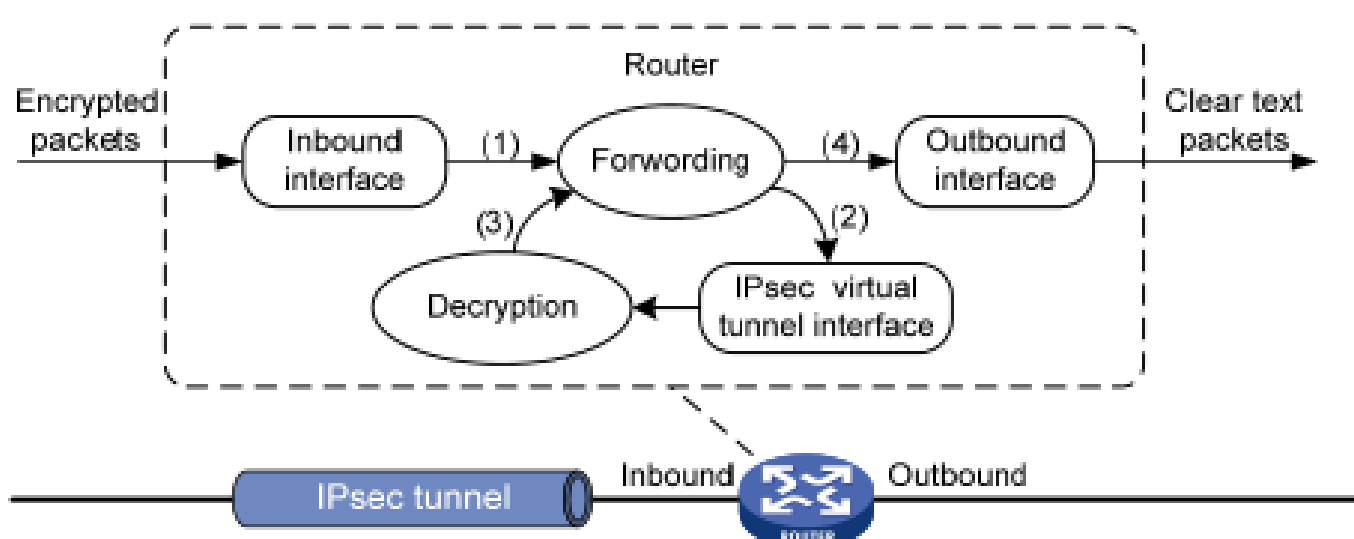


图 2.4 IPsec 虚拟隧道接口对报文进行解封装的过程

- (1) Router 将从入接口接收到的 IP 密文送到转发模块进行处理；
- (2) 转发模块识别到此 IP 密文的目的地为本设备的隧道接口地址且 IP 协议号为 AH 或 ESP 时，会将 IP 密文送到相对应的 IPsec 虚拟隧道接口进行解封装，将 IP 密文的外层 IP 头去掉，对内层 IP 报文进行解密处理。
- (3) IPsec 虚拟隧道接口完成对 IP 密文的解封装处理后，将 IP 明文重新送回

转发模块处理；

(4)转发模块进行第二次路由查询后，将 IP 明文从隧道的技术物理接口转发出去。

二、安全关联

1、定义

安全关联（Security Association，SA），是 IPsec 的基础。AH 和 ESP 都使用 SA，SA 是两个通信实体经过协商建立起来的一种提供安全服务的连接。它规定用来保护数据的 IPsec 协议类型，加密算法，认证方式，加密和认证密钥，密钥生存时间以及防重放攻击序列号等，位所承载的流量提供安全服务。SA 是一个单向的逻辑连接，在一次通信中，IPsec 需要建立两个 SA，一个用于进站通信，另外一个用于出站通信。

通过一个三元组参数可以唯一标识每个 SA，包括参数索引 SPI，源 IP 地址，目的 IP 地址和特定的安全协议（AH 和 ESP）。SA 只适用于点到点通信。

SPI 是一个 32 位证书，并且是为了唯一标识 SA 参胜的，SPI 在 AH 和 ESP 头中传输，所以，IPsec 数据包的接收方易于识别 SPI，并利用它连同源/目的 IP 地址和协议来搜索 SPD，以确定与该数据包相关联的 SA

2、SA 的功能

SA 所能够提供的安全服务取决于所选择的安全协议，SA 的工作模式，SA 终点和协议内所选择的服务。

AH 可以为接收端提供抗重播服务，防止拒绝服务攻击。当不需要或不允许使用数据的保密性时，最好使用 AH 协议。AH 也可以用于需要对 IP 头做认证服务的情形。AH 为 IP 数据流提供了高强度的密码认证，以确保被修改过的数据包可以被检查出来。

ESP 为流量可选择提供保密服务，保密服务的强度取决于 ESP 所使用的加密算法。ESP 也可以提供认证服务。使用 ESP SA 隧道模式可以加密内部 IP 头，隐藏流量的源/目的 IP 地址，进一步可以利用 ESP 填充字段隐藏数据包的真实长度。ESP 也可用于拨号方式的移动用户，在用户和企业之间建立隧道模式的 ESP SA。

3、SA 数据库（SAD）

IPsec 使用选择符选择应该使用的 SA，而选择符是根据 IP 层和传输层的信息标志生成的。IPsec 系统用中的安全策略数据库和安全联盟数据库与 SA 紧密相关。SPD 规定所有来之主机，安全网关等的 IP 包应该使用安全策略，SAD 包含每个 SA 的相关参数，它是将所有的 SA 以某种数据结构集中存储的列表。

（1）、选择符

选择符是从网络层包头和传输层帧头中提取出来的，由目的地址，源地址，名字，协议和上层端口组成，用于选择为包提供的安全服务

（2）、安全策略数据库（SPD）

SPD 是根据 IP 包的源地址、目的地址、入数据还是出数据等，规定以何种方式对 IP 包提供服务，是 SA 的基础。

SPD 的策略是有序的，对于出数据流或入数据流的三种处理方式如下：

- ①丢弃，不处理包，只是简单的丢弃
- ②绕过 IPsec，不需要 IPsec 保护包，生成普通的 IP 包送出
- ③应用 IPsec 对包提供保护，且 SPD 必须说明希望提供安全服务、协议和算法

（3）、安全联盟数据库（SAD）

SAD 中包含现有的 SA 条目，每个 SA 包括一个三元组，用于唯一标识这个 SA。该三元组包含一个 SPI，一个用于输入处理 SA 的源 IP 地址或一个用于处理 SA 的目的 IP 地址和一个特定的协议。一个 SAD 条目包含以下内容：

- ①本方序列号计数器：用于产生 AH 或 ESP 头的序列号字段，仅用于外出的数据包。
- ②对方序列号溢出标志：标识序列号计数器是否溢出。
- ③抗重放窗口：用于决定进入的 AH 或 ESP 数据包是否为重放的，仅用于进入数据包。
- ④AH 验证算法、密钥等
- ⑤ESP 加密、密钥等
- ⑥ESP 验证算法、密钥等
- ⑦SA 的生存期，表示 SA 能够存在的最长时间。
- ⑧运行模式：是传输模式还是隧道模式
- ⑨路径醉倒传输单元参数 PMTU：所考察的路径的 MTU 以及生存时间 TTL 变量

(4)、SA 的密钥管理

SA 的管理主要包括创建和删除,有以下两种管理方式:

- ①手工管理: SA 的内容由管理员手工指定,手工维护。但是,手工维护容易出错,而且手工建立的 SA 没有生存周期限制,有安全隐患。
- ②IKE 自动管理: 一般来说, SA 的自动建立和动态维护是通过 IKE 进行的。利用 IKE 创建和删除 SA。如果安全策略要求建立安全、保密的连接,但又不存在相应的 SA, IPsec 的内核会立刻启动 IKE 来协商 SA

三、AH 头认证

1、AH 简介

在 IP 协议中,验收 IP 数据报完整性是通过头部的校验和来保证的。这样,当修改 IP 头后,可以对修改过得 IP 头重新计算校验和并代替之间的校验和,从而让接受主机无法知道数据报已经修改。通过应用认证头协议可以增加 IP 数据包的安全性^[9]。

AH 为 IP 包提供数据完整性校验,身份认证和可选的抗重播保护,但是 AH 不对受保护的 IP 包加密。AH 的作用是 IP 数据流提供高强度的密码认证,以确保被修改过的数据报可以被检查出来。

AH 可单独使用,也可以与 ESP 结合使用,在隧道模式中嵌套使用。

1.AH 头格式

AH 被用来保证 IP 包在传输过程中是不被修改的,并且由指定发送人将它发送除去的新的非重播的数据包, AH 头格式如下表。2.1

表 2.1 AH 头格式

8	8	16bit
下一个头	载荷长度	保留
安全参数索引 (SPI)		
序列号		
认证数据 (可变)		

- ① 下一个头 (8bit), 指示下一个负载的协议的类型
- ② 载荷长度 (8bit), AH 的负载长度
- ③ 保留 (8bit), 供将来使用
- ④ 安全参数索引 SPI, SPI 是为了唯一标识 SA 而生成一个 32 位整数,

它包含在 AH 头标和 ESP 头标中,其值 1~255 被 IANA 留作将来使用,0 被保留,运用 SPI,在相同的源,目的节点的数据流可以建立多个 SA

- ⑤ 序列号 (32bit),单调增加的 32 为无符号整数,利用该域抵抗重发攻击
- ⑥ 认证数据,是一个长度可变的域,长度为 32 比特的整数倍,具体格式随认证算法变化儿不同。该认证数据也被称为数据报的完整性校验值。

2、AH 处理

下表 2.2 是一个标准数据包的格式

表 2.2 原始数据包格式

ver	hlen	TOS	Pkt len
ID		flgs	Frag offset
TTL	Proto=TCP	Header cksum	
Src IP address			
Dst IP address			
IP options(if present)			
TCP header (proto =6)			
TCP payload			

上表为我们常用的 IPv4 数据包的信息,其中 proto 字段描述了传输层的协议类型。

我们常见的传输层类型表如下表 2.3

表 2.3 传输层协议表

协议代码	协议描述
1	ICMP — 互联网控制消息协议
2	ICGP — 互联网组管理协议
4	IP within IP 一种类型的封装
6	TCP — 传输控制协议
17	UDP — 用户数据报协议
41	Ipv6 — 下一代 TCP/IP
47	GRE 协议 — 常规路由器封装用在 PPTP
50	Ipsec ESP — 封装安全负载
51	Ipsec AH— 头认证

AH 用于认证一但不对 IP 流量做加密,它提供主要的目的是确保我们是在和

我们想通信的主机之间通信，通过对传输的数据检测是否其被修改来防止攻击者捕捉了之前通讯的数据包，并藏是修改后重新发回给网络，让我们接受，这种攻击行为称为数据重演。

AH 认证是通过计算出 IP 包头中除 TTL 或头效验的所有字段的 hash 值，并将它存在新的 AH 头中的一起发送给另外一端来实现。

3、AH 报具体处理步骤：

（1）、对外出的数据包的处理

① 查找对应的 SA，更具待处理的数据包，构造出选择符（源 IP 地址，目的 IP 地址，协议号，通信端口），并以此选择符位索引检查的 SPI。加入按索引检查到的 SPI 条目，该分组应受到 AH 保护，则按 SPI 条目直接只指向的 SA 条目找到用以处理数据的 SA。如果 SPI 指向 SA 为空。则采用 IKE 协议协商新的 SA。

② 按 SA 条目给出的处理模式，在适当的地方插入 AH 头和外部 IP 头。在传输模式的 AH 实现中，带添加的 IP 头为原 IP 头，对于隧道模式，将重新构造新的 IP 头，添加到 AH 载荷前面。

③ 对 AH 载荷的相应字段进行填充。

④ 对 AH 处理后的数据报，重新计算 IP 头效验和。如果处理后的数据包的长度大于本地 MTC，则进行 IP 分段。处理完毕的 IPsec 分组被交给数据链路层或 IP 层重新路由。

（2）对进入数据包的处理

① 数据包重组，对于收到的数据包，查看是否是一个完整的受 AH 保护的数据包，如果得到一个数据包指示一个 IP 包的分段，则必须保留这个分段，直到收到属于该数据包的所有分段，并成功重组后，在进行后续处理。

② 查找 SA，三元组（SAID，目的 IP 地址，协议号，SPI），用于标识一个 SA。由待处理的 IPsec 数据包提取 SAID 魅力用它作为索引对 SADB 进行检索，找到相应的处理该数据包的 SA。如果没有找到，则丢弃该数据包，并将次事件记录于日志中。

③ 序列号检查，如果次数据包的序列号落在该活动 SA 的滑动窗口内，切不是一个重复收到的数据包，则表明此数据包是有效的，继续后续处理，否则丢弃该数据包，并将此记录于日志中。

④ 检查 ICV 字段的值，首先将 AH 头中的 ICV 字段保存下来，然后将

这个字段清零，按鉴别算法和鉴别密钥，与发送端相同的计算方式计算一个散列输出。该散列输出与保存的 ICV 相比较，如果一样，则通过完整性检查，否则丢弃该数据包，并将此记录于日志中。

⑤ 重构明文数据包，对传输模式的 AH 而言，将 AH 载荷的“下一载荷头”字段赋值予 IP 头的协议字段，去除 AH 封装，对得到的 IP 数据包重新计算 IP 头校验和。对于隧道埋没是的 AH 封装，内部 IP 头即是原 IP 头。因此恢复处理只需要除掉外部 IP 头，AH 头，便得到原明文 IP 数据包。

⑥ 对处理的合法性检查，ICV 校验完成后，应将该数据包的保护方式与 SA 指向的 SPI 条目的安全策略相比较，以检查安全实施的一致性。若相符，则继续后续处理，否则丢弃该数据包，并将此记录于日志中。

四、ESP 简介

ESP 为 IP 报文无连接的方式提供完整性校验，认证和加密服务，同时还可以提供防重放攻击保护。在选择期望得到的安全服务建立 SA 时，需要遵守如下约定 [5]：

- ① 同时支持完整性校验和身份认证
- ② 使用防重放攻击同时使用完整性校验和身份认证
- ③ 由接收端选着防重放攻击保护的使用
- ④ 加密独立与其他安全服务，但建议使用加密时同时使用完整性校验和身份认证

1、ESP 包格式

表 2.4 ESP 头格式

安全参数索引
序列号
初始化向量
载荷数据（长度可变）
0~255 个填充数据

填充长度	下一个头
认证数据（长度可变）	

① 安全参数索引（SPI），是一个任意的 32 位比特值，与目的 IP 地址和安全协议结合在一起，用来标识处理数据包的安全关联。SPI 一般在 IKE 交换过程中又目标住居选定。SPI 值为 0 表示预留给本地的特定的实现使用。

② 序列号（Sequence Number），与 AH 的序列号字段相同，为一个 32 比特字段的单项递增计数器

③ 初始化向量，包含于载荷数据字段，用于启动 ESP 的加密过程，是否需要初始化向量，由加密算法定。

④ 载荷数据（Payload Data），可变长字段。在这个域中，包含“下一个头”字段所说明的数据。

⑤ 填充项（Padding），填充项的使用是为了保证 ESP 的便捷适合于加密算法的需要

⑥ 填充长度（Pad Length）指出上面的填充项填充了多少字节的数据。通过填充长度，接收端可以恢复出载荷数据的真实长度。

⑦ 下一个头（NextHeader），8 比特字段，在传输模式下，是载荷中受保护的上层协议的编号。在隧道模式下封装时这个值是 4,表示 IP-in-IP, IPv6 下这个值位 41。

⑧ 认证数据（Authentication Data），字段的长度由选着的认证功能指定。它包含数据完整检验结果。

2、ESP 处理

对 ESP 来说，加密的数据包是已经认证的，需认证的数据包是未加密的。ESP 打不都采用对成密码体制加密数据，这是因为公钥密码系统的运算量要比对称密钥系统大得多^[12]。

（1）、对于发出数据包的具体处理步骤为：

① 使用相应的选择符查找安全数据库获取策略，其中包括 SPI，密钥等

② 生成或增加序列号，计算器初始化为 0,但发送由第一个数据包开始序列号开始递增，这样没个序列号都是非零的且唯一的单词递增的数

③ 对数据包进行加密，由 SA 指定的加密算法，如果选择认证，则加密要在认证前进行，加密不包含认证数据部分；

- ④ 计算机完整性校验值，包好 SPI，序列号，在和数据，填充项，填充长度和下一个头的密文数据等；
- ⑤ 重新计算机 ESP 前的 IP 头校验和，重新封装数据包。

（2）、对进入的数据包的处理步骤为

- ①若 IP 分组有被分片，则先重组分片包。
- ②使用三元组查询 SA,SA 决定是否检查序列号字段，若查询失败，则丢弃数据包；
- ③使用选择符在 SPD 中查询与数据包匹配的策略，根据策略检查是否满足 IPsec 的处理要求
- ④若 SA 指定需要进行认证，则检查数据的完整性，分别进行序列号验证和 ICV 认证；
- ⑤数据包进行解密

第三节 因特网密钥交换 IKE

一、IKE 定义

因特网密钥交换协议（IKE）能够为 AH 和 ESP 提供 SA 的自动协商，建立，保护的服务。它是 RFC2408 互联网安全联盟和密钥管理协议结合 Oakley 和 SKEME 等密钥交换技术构建的混合型密钥交换协议

IPsec 的实现应支持 IKE 协议，在受保护的方式下为 SA 协商和提供已认证的密钥材料。IKE 的实现可以支持协商 VPN，也可用于从远程访问安全主机或 IP 地址事先并不知道远程接入。

IKE 分为两个阶段，第一阶段，通信双方彼此建立一个以通过身份认证的安全保护的通道 IKE SA，使多有发起方和应答方之间的 IKE 通信信息都通过加密，完整性检查和认证的方法得到保护；第二阶段，位特定的英特网安全协议创建安全联盟^[6]。

二、IKE 的消息格式

1、ISAKMP 消息格式

IKE 实际定义了一个密钥交换，而 ISAKMP 仅提供了一个可由任意密钥交换协议使用的通用密钥交换框架，

ISAKMP 报文可以利用 UDP 或者 TCP，端口都是 500。一般情况下常用 UDP 协议。ISAKMP 消息采用固定的头格式，头格式之后携带可变长度的在和字段。

表 2.5 ISAKMP 的消息格式如下

8 字节				
发起者的 cookie				
响应着的 cookie				
下一载荷	主版本	副版本	交换类	标志
消息 ID				
消息长度				
消息载荷				

① 发起者 cookie，长度位 64bit。通过 cookie 可以让通信双方确认收到的 ISAKMP 报文是否由对方发送。如果验证此 cookie 字段和以前收到的 cookie 字段不同，则不论是发起放还是应答方，都丢弃此报文。应用这种机制可以防止拒绝服务攻击。

② 响应者 cookie，长度位 64bit

③ 下一载荷，长度位 64bit，目前定义了 13 种载荷

④ 主办本，长度为 4bit，表示 ISAKMP 协议的主坂本号

⑤ 副版本，长度为 4bit，表示 ISAKMP 协议的次版本号

⑥ 交换类型，长度为 8bit。表示报文所属的交换类型，目前定义了 5 种交换类型

⑦ 标志，长度为 8bit，目前只使用后三位，其他字段保留，用 0 填充

⑧ 消息 ID，长度为 32bit，包含由第二阶段协商的发起方生成的随机值，

次随机值可以唯一确定第二阶段的协议状态

- ⑨ 消息长度，表 IASKMP 整个报文的总长度，包括头部和若干载荷
- ⑩消息载荷

2、IKE 的消息格式

IKE 协议利用了 ISAKMP 提供的框架，结合 Oakley 和 SKEME 的密钥交换协议的优点。这种混合协议可以为 SA 的协商和密钥材料交换提供有效的安全性保护，既可以用于安全虚拟专用，也可以用于远程用户接入安全网络。

表 2.6 IKE 的消息格式

8 字节				
发起者的 cookie				
响应者的 cookie				
下一载荷	主版本	副版本	交换类型	标志
消息 ID				
消息长度				
10（nonce 载荷）	0（保留）		载荷长度	
KE 载荷数据				
0（none 载荷）	0（保留）		载荷长度	
nonce 载荷数据				

3、IKE 的认证方式

在 IKE 阶段的 DH 交换后，通信双方已经建立了一个共享密钥，但还没有通过身份认证，因此必须对 DH 的共享密钥进行认证^[14]。

IKE 有地中认证方式：

（1）、基于公开密钥的认证

这种认证交换通过用对方公开密钥加密身份，然后通过检查对方发来的该散列值做认证。正切的散列值证明对方能够解密用它自己的公开密钥加密的数据。使用公开密钥增加了密钥交换的安全性，因为攻击者必须攻破该 DH 交换和 RSA 交换。但是使用公开密钥做认证的缺点是计算机量相对较大，因为每一方都需要

做两次公开密钥的加密和解密。

（2）、基于修正过的公开密钥认证

这种认证方法具有认证凡是的很多优点,但用对成密钥算法替换了一些计算机代价很大的公开密钥算法。

（3）、基于预共享密钥的认证

在这种方法中,发起方和应答方必须有相同的预共享密钥,通常使用外带技术来协商密钥。在 IKE 主模式中,使用共享密钥需要已知对端 IP 地址,具有一定的局限性

（4）、基于数字签名的认证

这种认证交换使用协商好的数字签名算法做散列处理,散列算法应用在大多数已交换的参数上

4、IKE 在 IPsec 中的作用

①因为有了 IKE,IPsec 很多参数(如:密钥)都可以自动建立,降低了手工配置的复杂度。

②IKE 协议中的 DH 交换过程,每次的计算和产生的结果都是不相关的。每次 SA 的建立都运行

③DH 交换过程,保证了每个 SA 所使用的密钥互不相关。

④IPsec 使用 AH 或 ESP 报文头中的序列号实现防重放。此序列号是一个 32 比特的值,此数溢出后,为实现防重放,SA 需要重新建立,这个过程需要 IKE 协议的配合。对安全通信的各方身份的认证和管理,将影响到 IPsec 的部署。IPsec 的大规模使用,必须有 CA(Certificate Authority,认证中心)或其他集中管理身份数据的机构的参与。

⑤IKE 提供端与端之间动态认证。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/898016021050006065>